PURPOSE

The purpose of this procedure is to inform all Michigan Department of Health and Human Services (MDHHS) employees of the process to ensure that all suspected or actual privacy and security breaches, incidents and violations, including unauthorized or impermissible uses or disclosures, are appropriately identified, reported, documented, responded to, mitigated to the extent practicable, and evaluated for the implementation of breach notification procedures when required by law.

REVISION HISTORY

Issued: 11/02/2006
Revised: 01/01/2017
Reviewed:
Next Review: 01/01/2018

DEFINITIONS

Breach is the unauthorized acquisition, access, use, or disclosure of confidential information, FTI, PII, or PHI that compromises the security or privacy of the confidential information, FTI, PII, or PHI.

Confidential Information is information of a private nature that is protected by law from public disclosure, such as identifiable health information, social security numbers, etc.

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

Impermissible Use or Disclosure is the acquisition, access, use, or disclosure of confidential information, FTI, PII, or PHI in a manner not permitted under HIPAA or other applicable confidentiality laws that may or may not compromise the security or privacy of the confidential information, FTI, PII, or PHI.

PII is the acronym for Personally Identifiable Information. It is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

PHI is the acronym for Protected Health Information. It is information that can identify a person, contains health related data pertaining to that person and can be in any format: paper, verbal, electronic, etc.

FTI is the acronym for Federal Tax Information. It is information received from the Internal Revenue Service (IRS) pertaining to tax return information.

TIGTA is the acronym for Treasury Inspector General for Tax Administration. TIGTA provides independent oversight of IRS activities to prevent and detect fraud, waste, and abuse.

IRS Office of Safeguards is responsible for ensuring federal, state, and local agencies receiving federal tax information protect it as if the information remained in IRS's hands.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS to implement procedures to address suspected or actual privacy or security breaches, security incidents and violations, including unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI and create documented procedures defining the process for reporting such occurrences.

A reasonable security incident reporting mechanism for electronic confidential information, FTI, PII, or PHI will be tested by MDHHS on a regular basis.

A documented process that alerts appropriate authorities in the event that there is an information security threat, incident or other lapse in information security will be implemented.

MDHHS shall put in place procedures and processes to report, document and track breaches, security incidents, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI including but not limited to, recording incidents and how they were handled (for example what happened, when, cause, mitigation, prevention, who performed and when).

PROCEDURE

MDHHS Security Officer

The MDHHS Security Officer:

- Creates and implements a response and reporting system to support the reporting, mitigation and documentation of breaches, security incidences, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI.
- Notifies the Department of Technology, Management and Budget (DTMB) if a security incident involves an outside entity.
- Notifies the MDHHS supervisors and managers of policy updates and changes.

In the case of a security incident involving SSA-provided information:

- If MDHHS experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). MDHHS will provide updates as they become available to the SSA contact, as appropriate.

In the case of a security incident involving FTI:

- Notifies TIGTA and the IRS Office of Safeguards immediately, but no later than 24 hours after discovery of the suspected or known improper inspection or disclosure. Notification must not wait until an internal investigation is conducted. Contact information can be found in the IRS Publication 1075 (http://www.irs.gov/pub/irs-pdf/p1075.pdf Table 9 - TIGTA Field Division Contact Information).

- Conducts a post-incident review to ensure this incident response policy and procedure provides adequate guidance. Ensures workforce members with access to FTI receive training on this incident response policy and procedure.

Through collaboration with DTMB, makes department aware of:

- Viruses or other malicious software.
- State-wide threats to electronic confidential information, FTI, PII, or PHI.
- All other security threats.

MDHHS Security and Privacy Officers

The MDHHS Security and Privacy Officers must notify each other of security or privacy issues if they determine that an incident or issue could affect the other office (privacy or security).

The MDHHS Security and Privacy Officers are responsible for documenting and logging all breaches, security incidents, and unauthorized or impermissible uses or disclosures of confidential information, FTI PII, or PHI.

Department of Technology, Management and Budget/MDHHS Security Officer

DTMB and the MDHHS Security Officer must maintain open communication so that DTMB has a pathway to directly notify the MDHHS Security Officer of incidents that may impact electronic confidential information, FTI, PII, or PHI in MDHHS systems.

Division Director or Section Supervisor/Manager

The division director or section supervisor/manager must document and report all breaches, security incidences, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI.

The division director or section supervisor/manager must propagate recommendations, policy and procedure changes and security reminders to their areas. MDHHS managers and supervisors may receive updates by way of:

- MDHHS Privacy and Security Officer Policy Updates.
- MDHHS Security Officer Incident or Threat Updates.

Workforce Member

All workforce members must complete a DHHS-1422 Incident Report Form for each known or suspected incident and forward the completed form to the Privacy and Security Officers at MDHHSPrivacySecurity@michigan.gov. All breaches, security incidences, and unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI, threats or violations that affect or may affect the confidentiality, integrity or availability of FTI, PII, or PHI must be reported using the following procedures:

Users must notify DTMB Client Service Center in a timely manner for issues involving viruses, local attacks, Denial of Service (DOS) attacks, etc.

Incidents that involve confidential information, FTI, PII, or PHI must be immediately reported to (1) the immediate supervisor or manager of the workforce member's department and (2) the MDHHS Privacy and Security Officers. If the immediate supervisor or manager is unavailable, reporting processes should include the following steps:

- Notify local DTMB Client Service Center. The local helpdesk must notify DTMB if the incident effects or may affect other systems and networks.
- DTMB investigates and propagates recommended updates or fixes.
- DTMB notifies the MDHHS Security Officer if there is a viable threat to FTI, PII, or PHI.
- Incidents that must be reported include, but are not limited to:
    - Virus, worm or other malicious code attacks.
    - Network or system intrusions.
    - Persistent intrusion attempts from a particular entity.
    - Unauthorized access to or disclosure of: FTI, PII or PHI; FTI, PII or PHI-based system; or FTI, PII, or PHI-based networks.
    - FTI, PII, or PHI data loss due to disaster, failure or error.

- Unauthorized or impermissible uses or disclosures of confidential information, FTI, PII, or PHI in any format.

All instances of failures, outages or data loss that involve FTI or PHI must be reported to the MDHHS Security Officer.

All correspondence with outside authorities such as local police, FBI, IRS, SSA, media, etc. must go through the MDHHS Privacy and Security Officers.

REFERENCES

Public Act 452 of 2004

45 CFR 164.402

45 CFR 164.308(a)(6)

DTMB 1340.00.01, Acceptable Use of Information Technology.

DTMB 1340.00.110.01.01, Lost or Stolen State-Owned IT or Managed Equipment.

DTMB-0052, Lost or Stolen Equipment Report Form.

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Compliance Office MDHHSPrivacySecurity@michigan.gov.